PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-115162
(43)Date of publication of application : 21.04.2000

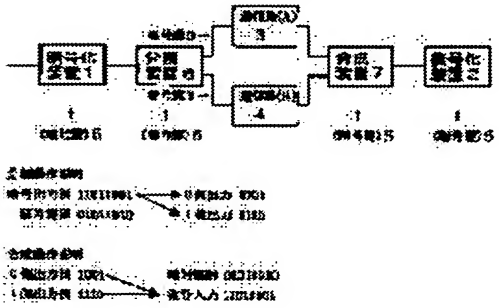
(51)Int.Cl. H04L 9/38
G09C 1/00

(21)Application number : 10-300314
(22)Date of filing : 08.10.1998

(71)Applicant : KODO IDO TSUSHIN SECURITY GIJUTSU KENKYUSHO:KK
(72)Inventor : KOYAMA OSAMU

(54) SECURE COMMUNICATION EQUIPMENT AND STORAGE DEVICE

(57)Abstract:
PROBLEM TO BE SOLVED: To make the eavesdropping of secret information difficult and to eliminate the danger of being deciphered any information is eavesdropped.
SOLUTION: After digitizing the secret information to be sent and converting it to a bit string, the bit string is ciphered by a cipher key 5 by a ciphering device 1 and then, divided into two data in a division device 6. The two data are separately sent to a communication path (A) 3 and the communication path (B) 4. The two communication paths can be cable communication paths, the combination of cable and radio communication paths, the different channels of the radio communication path or the same channel of different time. After synthesizing the two ciphered data by using the cipher key in a synthesizer 7 on a reception side, they are restored to one plain sentence in a deciphering device 2. Ciphering and division (synthesis and deciphering) can be integrated. By a similar method, the data can be divided into two and stored in two storage devices or the different areas of the same storage device. Three or more communication paths or storage devices can be used as well. By dividing the data by the cipher key and transmitting them, even when a part is eavesdropped, the danger of being deciphered is eliminated unless all is eavesdropped.



LEGAL STATUS

[Date of request for examination] 24.03.2000
[Date of sending the examiner's decision of rejection] 17.02.2004
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision

of rejection]
[Date of extinction of right]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1] The secure communication device characterized by providing the division means which divides information into two or more meaningless data if independent, and a transmitting means to send each data separately by two or more channels.
[Claim 2] The secure communication device according to claim 1 characterized by establishing an encryption means to divide data into said division means at plurality according to an encryption key.
[Claim 3] Said encryption means is a secure communication device according to claim 2 characterized by having a means to digitize transmit data and to change into a bit string, and a means to divide said bit string into two or more bit strings according to said encryption key.
[Claim 4] The secure communication device according to claim 2 characterized by establishing a receiving means to receive two or more encryption data separately from two or more channels, and a decode means to decode two or more received encryption data to one plaintext with a decode key.
[Claim 5] Secure storage characterized by providing the division means which divides information into two or more meaningless data if independent, and a write-in means to store each data in the storage region where the plurality of two or more storage or one storage differs.
[Claim 6] Secure storage according to claim 5 characterized by establishing an encryption means to divide data into said division means at plurality according to an encryption key.
[Claim 7] Said encryption means is secure storage according to claim 6 characterized by having a means to digitize a write data and to change into a bit string, and a means to divide said bit string into two or more bit strings according to said encryption key.
[Claim 8] The secure store according to claim 6 separately characterized by establishing the read-out means which reads two or more encryption data, and a decode means to decode two or more read encryption data to one plaintext with a decode key from the storage region where the plurality of said two or more stores or one store differs.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention relates to the secure communication device and store which divided secret information into plurality and raised security especially about a secure communication device and a store.

[0002]
[Description of the Prior Art] Conventionally, the means of communications or the storage means which raised security is used for electronic commerce and the exchange of secret information. Data are enciphered by the cryptographic key and it transmits through the channel of a cable or wireless, and the received encryption data are decoded using a decode key, and the plaintext of a basis is obtained. Or the enciphered data were written in the store, the store was carried, the data read from the store were decoded with the decode key, and the plaintext of a basis has been obtained. It is transmitted through one channel, and a cipher is stored in one storage, and is kept and carried.
[0003] Drawing 5 is the block diagram of conventional secret communication equipment. In drawing 5 , encryption equipment 1 is equipment which enciphers restricted data with an encryption key. A channel 10 is a channel of wireless or a cable. Decryption equipment 3 is equipment which decodes a cipher with a decode key and is returned to a plaintext. Even if a cipher is intercepted in a channel 10, if there is no decode key, it will be difficult to decode a cipher and a communicative secret will be secured.
[0004]
[Problem(s) to be Solved by the Invention] However, the enciphered data have risk of decoding with a certain means. Since it has gathered except [all] the decode key when a communication link is monitored or storage suits a theft, it is the problem of time amount that a part is also decoded. Moreover, when a decode key is stolen, there is a problem that all secret information will leak.
[0005] This invention solves the above-mentioned conventional problem, and it aims at making it not abused, unless all of the data divided even if it was in tapping and a theft encounter tapping and a theft while it makes informational tapping and a theft difficult by dividing secret information into plurality.
[0006]
[Means for Solving the Problem] In order to solve the above-mentioned technical problem, in this invention, it considered as the configuration possessing the division means which divides a secure communication device into two or more data which are meaningless if independent for information, and a transmitting means to send each data separately by two or more channels. When sending by channel which is different although two or more channels in this case are the same wireless besides in the case of a physically different channel, the case where it sends to time amount which is physically different also by the same channel is included. Thus, while being able to make difficult tapping of the information into which the channel was divided by having constituted, a secret is kept unless all that were divided even if intercepted are intercepted.
[0007] Moreover, an encryption means to divide data into a division means at plurality according to an encryption key was established. Thus, by having constituted, even if all are intercepted, as long as there is no cryptographic key, data cannot be reconfigurated.
[0008] Moreover, the encryption means was considered as the configuration which has a means to digitize transmit data and to change into a bit string, and a means to divide a bit string into two or more bit strings according to an encryption key. Thus, while being able to make informational tapping difficult by having constituted, even if intercepted, as long as there is no encryption key, the data divided into plurality cannot be reconfigurated.
[0009] Moreover, a receiving means to receive two or more encryption data separately from two or more channels, and a decode means to decode two or more received encryption data to one plaintext with a decode key were established. Thus, by having constituted, two or more divided encryption data can be easily reconfigurated with a decode key.
[0010] Moreover, it considered as the configuration possessing the division means which divides a secure store into two or more data which are meaningless if independent for information, and a write-in means to store each data in the storage region where the plurality of two or more stores or one store differs. Thus, while dividing storage and being able to make informational surreptitious use difficult by having constituted, insurance is securable unless all are stolen, even if some divided storage is in a theft.

[0011] Moreover, an encryption means to divide data into a division means at plurality according to an encryption key was established. Thus, by having constituted, as long as there is no encryption key, the data divided into plurality cannot be reconfigurated.
[0012] Moreover, the encryption means was considered as the configuration which has a means to digitize a write data and to change into a bit string, and a means to divide a bit string into two or more bit strings according to an encryption key. Thus, by having constituted, as long as there is no encryption key, the data divided into plurality cannot be reconfigurated.
[0013] Moreover, the read-out means which reads two or more encryption data, and a decode means to decode two or more read encryption data to one plaintext with a decode key were separately established from the storage region where the plurality of two or more stores or one store differs. Thus, by having constituted, it can reconfigurate easily with a decode key, keeping the secret of two or more divided encryption data.
[0014]
[Embodiment of the Invention] Invention of this invention according to claim 1 is a secure communication device possessing the division means which divides information into two or more meaningless data if independent, and a transmitting means to send each data separately by two or more channels, and has an operation of dividing a channel and making tapping difficult.
[0015] In a secure communication device according to claim 1, invention of this invention according to claim 2 establishes an encryption means to divide data into said division means at plurality according to an encryption key, and has an operation of an encryption key dividing data into plurality and making reconstruction difficult.
[0016] In a secure communication device according to claim 2, invention of this invention according to claim 3 has a means for said encryption means to digitize transmit data and to change into a bit string, and a means to divide said bit string into two or more bit strings according to said encryption key, and has an operation of an encryption key dividing data into plurality in digital one, and making reconstruction difficult.
[0017] Invention of this invention according to claim 4 has an operation of establishing a receiving means to receive two or more encryption data separately from two or more channels, and a decode means to decode two or more received encryption data to one plaintext with a decode key, and reconfigurating two or more divided encryption data with a decode key, in a secure communication device according to claim 2.
[0018] Invention of this invention according to claim 5 is the secure storage possessing the division means which divides information into two or more meaningless data if independent, and a write-in means to store each data in the storage region where the plurality of two or more storage or one storage differs, and has an operation of making decode of the data of the divided storage difficult.
[0019] In a secure store according to claim 5, invention of this invention according to claim 6 establishes an encryption means to divide data into said division means at plurality according to an encryption key, and has an operation of an encryption key dividing data into plurality and making reconstruction difficult.
[0020] In a secure store according to claim 6, invention of this invention according to claim 7 has a means for said encryption means to digitize a write data and to change into a bit string, and a means to divide said bit string into two or more bit strings according to said encryption key, and has an operation of an encryption key dividing data into plurality in digital one, and making reconstruction difficult.
[0021] Invention of this invention according to claim 8 has an operation of establishing the read-out means which reads two or more encryption data, and a decode means to decode two or more read encryption data to one plaintext with a decode key, separately, and reconfigurating two or more divided encryption data with a decode key from the storage region where the plurality of said two or more storage or one storage differs, in secure storage according to claim 6.
[0022] Hereafter, the gestalt of operation of this invention is explained to a detail, referring to drawing 1 - drawing 4 .
[0023] (Gestalt of the 1st operation) After the gestalt of operation of the 1st of this invention digitizes confidential information to send and changes it into a bit string, it is a secure communication device which enciphers, divides one cipher into two data, compounds and decrypts two ciphers which received each through delivery and a separate channel separately by two channels to one cipher, and is restored to one plaintext.
[0024] Drawing 1 is the system configuration Fig. of the secure communication device of the gestalt of operation of the 1st of this invention. In drawing 1 , encryption equipment 1 is equipment which enciphers a plaintext by the cryptographic key 5. Division equipment 6 is equipment which divides one cipher into two by the cryptographic key 5. A synthesizer unit 7 is equipment which compounds the reception encryption sentence divided into two to one cipher by the cryptographic key 5. Decryption equipment 2 is equipment which returns

the cipher compounded by one to a plaintext by the cryptographic key 5. A cryptographic key 5 is an encryption decryption common key. A channel (A) 3 is the 1st channel. A channel (B) 4 is the 2nd channel.
[0025] Actuation of the secure communication device of the gestalt of operation of the 1st of this invention constituted as mentioned above is explained using drawing 1 . With the equipment which is not illustrated, information to send is digitized and it changes into bit-string data. The changed bit-string data is enciphered with encryption equipment 1 using a cryptographic key 5. So far, it is the same as conventional equipment, and existing equipment can be used.
[0026] With division equipment 2, when dividing information into plurality, the technique of encryption is applied. 1 bit (a cryptographic key 5 is repeated and used) of bit strings of a cryptographic key 5 is made to correspond at a time to the enciphered bit string, when the bit of a cryptographic key is "0", it outputs to a channel (A) 3 side, and when the bit of a cryptographic key is "1", it outputs to a channel (B) 4 side. After all, the cipher divided into two is acquired from one data.
[0027] In a channel (A) 3, the bit of a cryptographic key transmits the division data corresponding to "0." In a channel (B) 4, the bit of a cryptographic key transmits the division data corresponding to "1." Thus, information is divided into two or more data, and each is separately sent by two or more channels. When sending by channel which is different although two or more channels in this case are the same wireless besides in the case of a physically different channel, the case where it sends to time amount which is physically different also by the same channel is included.
[0028] In a receiving side, actuation contrary to a transmitting side is performed, composition and a decryption of two received data are performed, and the original message is taken out. Encryption data are received from a channel (A) 3 and a channel (B) 4, and two encryption data are compounded using a cryptographic key 5 with a synthesizer unit 7. 1 bit of bit strings of a cryptographic key 5 is made to correspond at a time, to two encryption bit strings which received, when the bit of a cryptographic key is "0", it inputs from a channel (A) 3 side, and when the bit of a cryptographic key 5 is "1", it inputs from a channel (B) 4 side. With decryption equipment 2, the compound bit string is decoded using a cryptographic key 5, and it restores to a plaintext.
[0029] Thus, since encryption data are divided into two data and it transmits using the technique of encryption, even if it is going to intercept and decode one division data, only meaningless data are completely obtained but there is no risk of secret data being abused.
[0030] In addition, although the example which divided division and composition by encryption and decryption was explained, cryptocommunication is possible, even if it omits encryption and a decryption and uses only division and composition. A cryptographic key is used for the reverse by encryption and decryption, and it is good for it also as mere mutual division, not using a cryptographic key by division and composition. Moreover, although the example of a common private key method was explained about the cryptographic key, it is also possible to use a common private key for division composition, and to use a public key system for an encryption decryption.
[0031] Although the example using two channels was explained, it is clear that three or more channels may be used. When dividing into four, a distribution place is decided corresponding to 2 bits of a key. It is possible to divide into 2n by using n bits of a key similarly. What is necessary is to use n bits of a key, to see this as a binary number to divide into 2n-1 and the number between 2n, and just to ignore, when it is more than a number to divide this number. For example, when dividing into three, it is the case of n= 2, and the list of the bit of a key has four, 00, 01, 10, and 11. In a decimal number, the time of the bit list 11 of the key which are 0, 1, 2, and 3 and is three or more is disregarded, and a swing part injury of the three remaining is possible. In a receiving side, this can be performed conversely and can be compounded. A problem is not produced also when compounding by the receiving side, since it is a common key system.
[0032] as mentioned above, with the gestalt of operation of the 1st of this invention After digitizing information to send a secure communication device and changing into a bit string, Since encryption processing of this was carried out and it was made the configuration which divides into two data after that, decodes after compounding to one two ciphers which received each through delivery and a separate channel separately by two channels, and restores one plaintext Informational tapping becomes difficult, and decryption is impossible even if it intercepts one of the two of division.
[0033] (Gestalt of the 2nd operation) After the gestalt of operation of the 2nd of this invention digitizes confidential information to send and changes it into a bit string, it is a secure communication device which restores two ciphers which performed encryption processing and data division as one, and received each through delivery and a separate channel separately by two channels to one plaintext.

[0034] Drawing 2 is the system configuration Fig. of the secure communication device of the gestalt of operation of the 2nd of this invention. In drawing 2 , encryption equipment 1 is equipment which divides the data of the plaintext which transmits into two while enciphering with an encryption key. Decryption equipment 2 is equipment which returns the reception encryption data divided into two to one plaintext. A channel (A) 3 is the 1st channel. A channel (B) 4 is the 2nd channel.
[0035] Actuation of the secure communication device of the gestalt of operation of the 1st of this invention constituted as mentioned above is explained using drawing 2 . With the equipment which is not illustrated, information to send is digitized and it changes into bit-string data. The changed bit-string data is divided into two at the same time it enciphers with encryption equipment 1 using a cryptographic key.
[0036] As an example of the approach of performing by summarizing encryption and division, the example using a DES method famous as a block cipher is shown. Although DES is processed every 64 bits, by the way, it takes out at a time 32 bits of one side on either side which is the final output, and divides them into two (refer to drawing 3). This is made reverse and composition and decode are performed.
[0037] One division encryption data are transmitted in a channel (A) 3. The division encryption data of another side are transmitted in a channel (B) 4. Thus, information is divided into two or more data, and each is separately sent by two or more channels. When sending by channel which is different although two or more channels in this case are the same wireless besides in the case of a physically different channel, the case where it sends to time amount which is physically different also by the same channel is included.
[0038] In a receiving side, actuation contrary to a transmitting side is performed, composition and a decryption of two received data are performed, and the original message is taken out. a decryption — equipment — two — **** — a channel — (— A —) — three — a channel — (— B —) — four — from — encryption — data — receiving — having received — two — a ** — encryption — a bit string — a cryptographic key — using — compounding — at the same time — decoding — a plaintext — restoring .
[0039] Thus, using the technique of encryption, encryption and division are performed as one and composition and a decryption are performed as one. Since one data is divided into encryption and coincidence and it transmits, even if it is going to intercept and decode one division data, only meaningless data are completely obtained but there is no risk of secret data being abused. Although the example using two channels was explained, it is clear that three or more channels may be used.
[0040] as mentioned above, with the gestalt of operation of the 2nd of this invention After digitizing information to send a secure communication device and changing into a bit string, Since it was made the configuration which restores one plaintext from two ciphers which performed encryption processing and data division for this as one, and received each through delivery and a separate channel separately by two channels, informational tapping becomes difficult, and decryption is impossible even if it intercepts one of the two of division.
[0041] (Gestalt of the 3rd operation) The gestalt of operation of the 3rd of this invention is secure storage which restores two ciphers which divided into two data, stored each in two storage separately, and were read from separate storage to one plaintext, carrying out encryption processing, after digitizing confidential information and changing into a bit string.
[0042] Drawing 4 is the block diagram of the secure storage of the gestalt of operation of the 3rd of this invention. In drawing 4 , encryption equipment 1 is equipment which enciphers the data of the plaintext to memorize with an encryption key. Decryption equipment 2 is equipment which returns encryption data to a plaintext. Storage (A) 8 is the 1st storage. Storage (B) 9 is the 2nd storage.
[0043] Actuation of the secure storage of the gestalt of operation of the 3rd of this invention constituted as mentioned above is explained using drawing 4 . In a store side, with the equipment which is not illustrated, the confidential information to memorize is digitized and it changes into bit-string data. The changed bit-string data is divided while enciphering with encryption equipment 1 using a cryptographic key. Although simple mutual division may be used when dividing information into two, encryption and division are performed as one like the gestalt of the 2nd operation using a cryptographic key. In this way, the cipher divided into two is acquired from one data.
[0044] One division data are memorized in a store (A) 8. The division data of another side are memorized in a store (B) 9. Thus, information is divided into two data and each is separately stored in two storage. Physically different storage and a physically different storage are sufficient as two storage in this case, or the storage region where one storage differs from storage is sufficient as it. Although it is safer to use physically different storage and a physically different storage, if the storage region is secret even when using the field where one storage differed from storage, there will be no problem according to rank in safety.

[0045] In a read-out side, actuation contrary to a store side is performed, composition and decode of two read-out.data are performed, and the original message is taken out. a store — (— A —) — eight — a store — (— B —) — nine — from — encryption — data — reading — decryption equipment 2 — a cryptographic key — using — two encryption data — composition — decoding — the plaintext of a basis — restoring .
[0046] Thus, since encryption data are divided and memorized to two data, even if it is going to steal and decode the store which stored one division data, only meaningless data are completely obtained but there is no risk of secret data being decoded. Therefore, secret data can be carried or kept safely.
[0047] In addition, it divides into three or more encryption data, and you may make it memorize to three or more storage like the case of a communication link. Moreover, encryption, division and composition, and decode may be separated like the gestalt of the 1st operation.
[0048] as mentioned above, with the gestalt of operation of the 3rd of this invention Carrying out encryption processing of this, after digitizing the information which memorizes a secure store and changing into a bit string Since it considered as the configuration which restores two ciphers which divided into two data, stored each in two storage separately, and were read from separate storage to one plaintext While making the theft of the whole information difficult, even if some storage is in a theft, unless all storage and decode keys are stolen, a secret does not leak.
[0049]
[Effect of the Invention] As mentioned above, since it considered as the configuration which possesses the division means which divides a secure communication device into two or more meaningless data for information if independent, and a transmitting means to send each data separately according to two or more channels, in this invention, while dividing a channel and being able to make informational tapping difficult, the effectiveness of not being abused unless all are intercepted, even if some divided data are intercepted is acquired.
[0050] Moreover, since an encryption means to divide data into a division means at plurality according to an encryption key was established, as long as there is no encryption key, the effectiveness that the data divided into plurality cannot be reconfigurated is acquired.
[0051] Moreover, since the encryption means was considered as the configuration which has a means to digitize transmit data and to change into a bit string, and a means to divide a bit string into two or more bit strings according to an encryption key, as long as there is no encryption key, the effectiveness that the data divided into plurality cannot be reconfigurated is acquired.
[0052] Moreover, since a receiving means to receive two or more encryption data separately from two or more channels, and a decode means to decode two or more received encryption data to one plaintext with a decode key were established, the effectiveness that two or more divided encryption data can be easily reconfigurated with a decode key is acquired.
[0053] Moreover, since it considered as the configuration possessing the division means which divides a secure store into two or more meaningless data for information if independent, and a write-in means store each data in the storage region where the plurality of two or more stores or one store differs, while divide a store and being able to make informational tapping difficult, the effectiveness are not abused unless all are stolen, even if some divided stores are in a theft is acquired.
[0054] Moreover, since an encryption means to divide data into a division means at plurality according to an encryption key was established, as long as there is no encryption key, the effectiveness that the data divided into plurality cannot be reconfigurated is acquired.
[0055] Moreover, since an encryption means has a means to digitize a write data and to change into a bit string, and a means to divide a bit string into two or more bit strings according to an encryption key, unless it has an encryption key, the effectiveness that the data divided into plurality cannot be reconfigurated is acquired.
[0056] Moreover, since the read-out means which reads two or more encryption data, and a decode means to decode two or more read encryption data to one plaintext with a decode key were separately established from the storage region where the plurality of two or more stores or one store differs, the effectiveness that two or more divided encryption data can be easily reconfigurated with a decode key is acquired.

[Translation done.]

* NOTICES *

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1] The block diagram of the secure communication device of the gestalt of operation of the 1st of this invention,
[Drawing 2] The block diagram of the secure communication device of the gestalt of operation of the 2nd of this invention,
[Drawing 3] The block diagram of the encryption equipment used with the secure communication device of the gestalt of operation of the 2nd of this invention,
[Drawing 4] The block diagram of the secure storage of the gestalt of operation of the 3rd of this invention,
[Drawing 5] It is the conventional cryptocommunication structure-of-a-system Fig.
[Description of Notations]
1 Encryption Equipment
2 Decryption Equipment
3 Channel (A)
4 Channel (B)
5 Cryptographic Key
6 Division Equipment
7 Synthesizer Unit
8 Storage (A)
9 Storage (B)
10 Channel

[Translation done.]

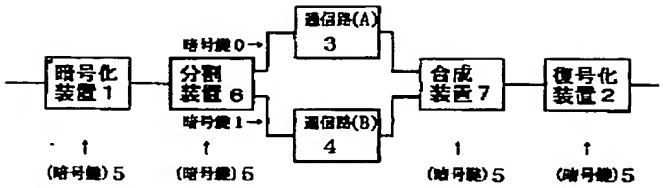
* NOTICES *

JPO and NCIPI are not responsible for any
damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DRAWINGS

[Drawing 1]



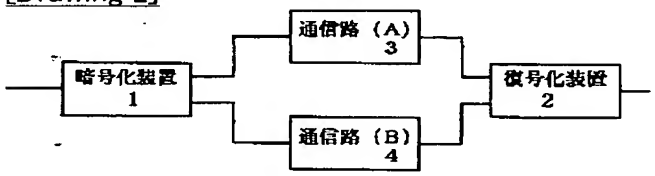
分割動作説明

暗号出力例 11011001 → 0側出力 1001
暗号鍵例 01011010 → 1側出力 1110

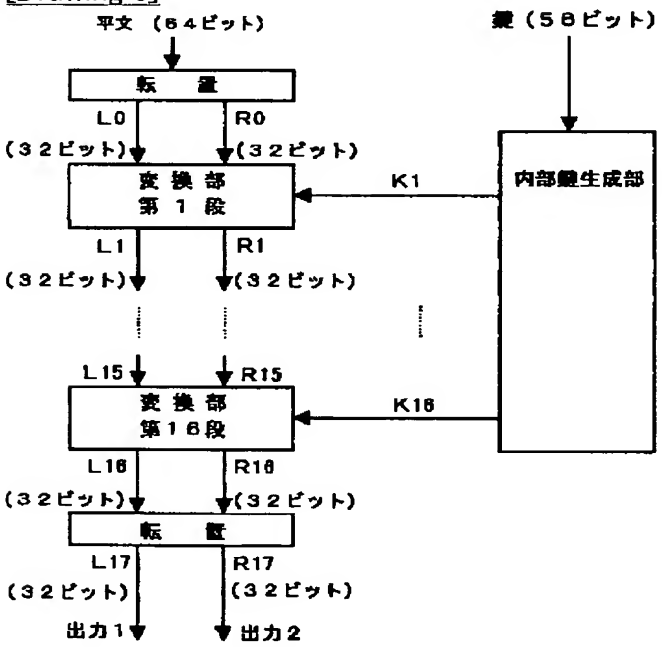
合成動作説明

0側出力例 1001
1側出力例 1110
暗号鍵例 01011010
復号入力 11011001

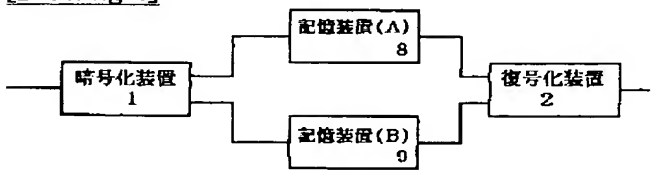
[Drawing 2]



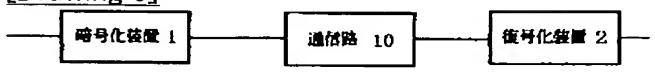
[Drawing 3]



[Drawing 4]



[Drawing 5]



[Translation done.]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号
特開2000－115162
（P2000－115162A）
(43)公開日　平成12年４月21日(2000.4.21)

(51)Int.Cl.⁷		識別記号	FI			テーマコード（参考）
Ｈ０４Ｌ	9/38		Ｈ０４Ｌ	9/00	６９１	５Ｊ１０４
Ｇ０９Ｃ	1/00	６６０	Ｇ０９Ｃ	1/00	６６０Ｆ	９Ａ００１

審査請求　未請求　請求項の数８　ＦＤ　（全６頁）

(21)出願番号　特願平10－300314

(22)出願日　平成10年10月８日(1998.10.8)

(71)出願人　597174182
株式会社高度移動通信セキュリティ技術研究所
神奈川県横浜市港北区新横浜三丁目20番地８

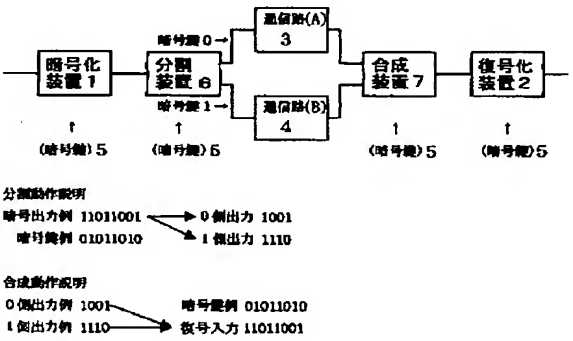
(72)発明者　小山　修
神奈川県横浜市港北区新横浜三丁目20番地８号　株式会社高度移動通信セキュリティ技術研究所内

(74)代理人　100099254
弁理士　役　昌明　（外１名）

Ｆターム(参考)　5J104 AA01 AA03 AA34 JA04 NA02 PA10
9A001 EE03 JJ18 JJ67 KK56 LZ03

(54)【発明の名称】　セキュア通信装置及び記憶装置

(57)【要約】
【課題】　秘密の情報の盗聴を困難にするとともに、全部の情報が盗聴されない限り暗号解読されるおそれもないようにする。
【解決手段】　送りたい秘密の情報をデジタル化してビット列に変換した後、暗号化装置１により、ビット列を暗号鍵５で暗号化した後、分割装置６で２つのデータに分割する。２つのデータを、通信路（Ａ）３と通信路（Ｂ）４で別々に送る。２つの通信路は、有線の通信路でも、有線と無線の通信路の組合せでも、無線の通信路の異なるチャンネルでも、異なる時間の同じチャンネルでもよい。受信側の合成装置７で暗号鍵を使って２つの暗号化データを合成した後、復号化装置２で１つの平文に復元する。暗号化と分割（合成と復号）は一体としてもよい。同様の方法でデータを２つに分け、２つの記憶装置または同じ記憶装置の異なる領域に記憶してもよい。３つ以上の通信路または記憶装置を使うことも可能である。データを暗号化鍵で分割して送信することで、一部が盗聴されても、全部が盗聴されない限り、暗号解読されるおそれはない。



1

【特許請求の範囲】

【請求項１】　情報を単独では意味のない複数のデータに分ける分割手段と、それぞれのデータを複数の通信路で別々に送る送信手段とを具備することを特徴とするセキュア通信装置。

【請求項２】　前記分割手段に、暗号化鍵に応じてデータを複数に分割する暗号化手段を設けたことを特徴とする請求項１記載のセキュア通信装置。

【請求項３】　前記暗号化手段は、送信データをデジタル化してビット列に変換する手段と、前記ビット列を前記暗号化鍵に応じて複数のビット列に分割する手段とを有することを特徴とする請求項２記載のセキュア通信装置。

【請求項４】　複数の通信路から別々に複数の暗号化データを受信する受信手段と、受信した複数の暗号化データを復号鍵により１つの平文に復号する復号手段とを設けたことを特徴とする請求項２記載のセキュア通信装置。

【請求項５】　情報を単独では意味のない複数のデータに分ける分割手段と、それぞれのデータを複数の記憶装置または１つの記憶装置の複数の異なる記憶領域に格納する書込手段とを具備することを特徴とするセキュア記憶装置。

【請求項６】　前記分割手段に、暗号化鍵に応じてデータを複数に分割する暗号化手段を設けたことを特徴とする請求項５記載のセキュア記憶装置。

【請求項７】　前記暗号化手段は、書込データをデジタル化してビット列に変換する手段と、前記ビット列を前記暗号化鍵に応じて複数のビット列に分割する手段とを有することを特徴とする請求項６記載のセキュア記憶装置。

【請求項８】　前記複数の記憶装置または１つの記憶装置の複数の異なる記憶領域から別々に複数の暗号化データを読み出す読出手段と、読み出した複数の暗号化データを復号鍵により１つの平文に復号する復号手段とを設けたことを特徴とする請求項６記載のセキュア記憶装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、セキュア通信装置及び記憶装置に関し、特に、秘密の情報を複数に分けてセキュリティを高めたセキュア通信装置及び記憶装置に関する。

【０００２】

【従来の技術】従来、電子商取引や、秘密の情報のやり取りのため、セキュリティを高めた通信手段あるいは記憶手段が利用されている。データを暗号鍵で暗号化し、有線または無線の通信路を介して送信し、受信した暗号化データを復号鍵を使って復号し、もとの平文を得る。あるいは、暗号化したデータを記憶装置に書き込み、記憶装置を運搬し、記憶装置から読出したデータを復号鍵で復号して、もとの平文を得ている。暗号文は１つの通信路を介して送信され、１つの記憶装置に格納されて保管、運搬される。

2

【０００３】図５は、従来の秘密通信装置の構成図である。図５において、暗号化装置１は、秘密データを暗号化鍵で暗号化する装置である。通信路10は、無線あるいは有線の通信路である。復号化装置３は、復号鍵により暗号文を復号して平文に戻す装置である。通信路10において暗号文が盗聴されても、復号鍵がなければ暗号文を解読することは困難であり、通信の秘密は確保される。

【０００４】

【発明が解決しようとする課題】しかし、暗号化したデータは、何らかの手段で解読される危険がある。通信が傍受されたり、記憶装置が盗難にあった場合は、復号鍵以外はすべて揃っているので、一部でも解読されるのは時間の問題である。また、復号鍵を盗まれた場合は、秘密の情報がすべて漏れてしまうという問題がある。

【０００５】本発明は、上記従来の問題を解決し、秘密の情報を複数に分けることにより情報の盗聴、盗難を困難にするとともに、盗聴、盗難にあっても分割したデータの全部が盗聴、盗難に遭わない限り悪用されないようにすることを目的とする。

【０００６】

【課題を解決するための手段】上記の課題を解決するために、本発明では、セキュア通信装置を、情報を単独では意味のない複数のデータに分ける分割手段と、それぞれのデータを複数の通信路で別々に送る送信手段とを具備する構成とした。この場合の複数の通信路とは、物理的に異なる通信路の場合の他、同じ無線であるが異なるチャンネルで送る場合、あるいは物理的に同じ通信路でも異なる時間に送る場合を含む。このように構成したことにより、通信路が分かれた情報の盗聴を困難にできるとともに、盗聴されても分割した全部が盗聴されない限り秘密は守られる。

【０００７】また、分割手段に、暗号化鍵に応じてデータを複数に分割する暗号化手段を設けた。このように構成したことにより、全部が盗聴されても暗号鍵がない限りデータを再構成できない。

【０００８】また、暗号化手段は、送信データをデジタル化してビット列に変換する手段と、ビット列を暗号化鍵に応じて複数のビット列に分割する手段とを有する構成とした。このように構成したことにより、情報の盗聴を困難にできるとともに、盗聴されても、暗号化鍵がない限り複数に分割されたデータを再構成できない。

【０００９】また、複数の通信路から別々に複数の暗号化データを受信する受信手段と、受信した複数の暗号化データを復号鍵により１つの平文に復号する復号手段とを設けた。このように構成したことにより、分割された複数の暗号化データを復号鍵により容易に再構成でき

る。

【００１０】また、セキュア記憶装置を、情報を単独では意味のない複数のデータに分ける分割手段と、それぞれのデータを複数の記憶装置または１つの記憶装置の複数の異なる記憶領域に格納する書込手段とを具備する構成とした。このように構成したことにより、記憶装置を分けて情報の盗用を困難にできるとともに、分割した一部の記憶装置が盗難にあっても全部が盗まれない限り安全が確保できる。

【００１１】また、分割手段に、暗号化鍵に応じてデータを複数に分割する暗号化手段を設けた。このように構成したことにより、暗号化鍵がない限り複数に分割されたデータを再構成できない。

【００１２】また、暗号化手段は、書込データをデジタル化してビット列に変換する手段と、ビット列を暗号化鍵に応じて複数のビット列に分割する手段とを有する構成とした。このように構成したことにより、暗号化鍵がない限り複数に分割されたデータを再構成できない。

【００１３】また、複数の記憶装置または１つの記憶装置の複数の異なる記憶領域から別々に複数の暗号化データを読み出す読出手段と、読み出した複数の暗号化データを復号鍵により１つの平文に復号する復号手段とを設けた。このように構成したことにより、分割された複数の暗号化データの秘密を守りながら復号鍵により容易に再構成できる。

【００１４】

【発明の実施の形態】本発明の請求項１記載の発明は、情報を単独では意味のない複数のデータに分ける分割手段と、それぞれのデータを複数の通信路で別々に送る送信手段とを具備するセキュア通信装置であり、通信路を分けて盗聴を困難にするという作用を有する。

【００１５】本発明の請求項２記載の発明は、請求項１記載のセキュア通信装置において、前記分割手段に、暗号化鍵に応じてデータを複数に分割する暗号化手段を設けたものであり、暗号化鍵によりデータを複数に分割して再構成を困難にするという作用を有する。

【００１６】本発明の請求項３記載の発明は、請求項２記載のセキュア通信装置において、前記暗号化手段は、送信データをデジタル化してビット列に変換する手段と、前記ビット列を前記暗号化鍵に応じて複数のビット列に分割する手段とを有するものであり、暗号化鍵によりデータをデジタル的に複数に分割して再構成を困難にするという作用を有する。

【００１７】本発明の請求項４記載の発明は、請求項２記載のセキュア通信装置において、複数の通信路から別々に複数の暗号化データを受信する受信手段と、受信した複数の暗号化データを復号鍵により１つの平文に復号する復号手段とを設けたものであり、分割された複数の暗号化データを復号鍵により再構成するという作用を有する。

【００１８】本発明の請求項５記載の発明は、情報を単独では意味のない複数のデータに分ける分割手段と、それぞれのデータを複数の記憶装置または１つの記憶装置の複数の異なる記憶領域に格納する書込手段とを具備するセキュア記憶装置であり、分割された記憶装置のデータの解読を困難にするという作用を有する。

【００１９】本発明の請求項６記載の発明は、請求項５記載のセキュア記憶装置において、前記分割手段に、暗号化鍵に応じてデータを複数に分割する暗号化手段を設けたものであり、暗号化鍵によりデータを複数に分割して再構成を困難にするという作用を有する。

【００２０】本発明の請求項７記載の発明は、請求項６記載のセキュア記憶装置において、前記暗号化手段は、書込データをデジタル化してビット列に変換する手段と、前記ビット列を前記暗号化鍵に応じて複数のビット列に分割する手段とを有するものであり、暗号化鍵によりデータをデジタル的に複数に分割して再構成を困難にするという作用を有する。

【００２１】本発明の請求項８記載の発明は、請求項６記載のセキュア記憶装置において、前記複数の記憶装置または１つの記憶装置の複数の異なる記憶領域から別々に複数の暗号化データを読み出す読出手段と、読み出した複数の暗号化データを復号鍵により１つの平文に復号する復号手段とを設けたものであり、分割された複数の暗号化データを復号鍵により再構成するという作用を有する。

【００２２】以下、本発明の実施の形態について、図１～図４を参照しながら詳細に説明する。

【００２３】（第１の実施の形態）本発明の第１の実施の形態は、送りたい秘密情報をデジタル化してビット列に変換した後、暗号化し、１つの暗号文を２つのデータに分割し、それぞれを２つの通信路で別々に送り、別々の通信路を介して受信した２つの暗号文を１つの暗号文に合成し、復号化して１つの平文に復元するセキュア通信装置である。

【００２４】図１は、本発明の第１の実施の形態のセキュア通信装置のシステム構成図である。図１において、暗号化装置１は、暗号鍵５で平文を暗号化する装置である。分割装置６は、１つの暗号文を暗号鍵５で２つに分割する装置である。合成装置７は、２つに分割された受信暗号化文を暗号鍵５で１つの暗号文に合成する装置である。復号化装置２は、１つに合成された暗号文を暗号鍵５で平文に戻す装置である。暗号鍵５は、暗号化復号化共通鍵である。通信路（Ａ）３は、第１の通信路である。通信路（Ｂ）４は、第２の通信路である。

【００２５】上記のように構成された本発明の第１の実施の形態のセキュア通信装置の動作を図１を使って説明する。図示していない装置で、送りたい情報をデジタル化し、ビット列データに変換する。変換したビット列データを、暗号鍵５を使って暗号化装置１により暗号化す

る。ここまでは、従来の装置と同じであり、既存の装置を利用できる。

【００２６】分割装置２では、情報を複数に分割する時に、暗号化の手法を適用する。暗号化したビット列に対して、暗号鍵５のビット列（暗号鍵５を繰り返し利用する）を１ビットずつ対応させて、暗号鍵のビットが「０」の場合は、通信路（Ａ）３側に出力し、暗号鍵のビットが「１」の場合は、通信路（Ｂ）４側に出力する。結局、１つのデータから２つに分割された暗号文が得られる。

【００２７】通信路（Ａ）３では、暗号鍵のビットが「０」に対応する分割データを転送する。通信路（Ｂ）４では、暗号鍵のビットが「１」に対応する分割データを転送する。このように、情報を複数のデータに分け、それぞれを複数の通信路で別々に送る。この場合の複数の通信路とは、物理的に異なる通信路の場合の他、同じ無線であるが異なるチャンネルで送る場合、あるいは物理的に同じ通信路でも異なる時間に送る場合を含む。

【００２８】受信側では、送信側と逆の操作を行ない、２つの受信データの合成と復号化を行ない、元のメッセージを取り出す。通信路（Ａ）３と通信路（Ｂ）４から暗号化データを受信し、合成装置７で暗号鍵５を使って、２つの暗号化データを合成する。受信した２つの暗号化ビット列に対して、暗号鍵５のビット列を１ビットずつ対応させて、暗号鍵のビットが「０」の場合は通信路（Ａ）３側から入力し、暗号鍵５のビットが「１」の場合は通信路（Ｂ）４側から入力する。復号化装置２では、暗号鍵５を使って、合成したビット列を復号して平文に復元する。

【００２９】このようにして、暗号化の手法を使って、暗号化データを２つのデータに分割して送信するので、一方の分割データを盗聴して解読しようとしても、全く意味のないデータしか得られず、秘密のデータが悪用される危険はない。

【００３０】なお、暗号化と復号化で分割と合成を分けた例を説明したが、暗号化と復号化を省略して、分割と合成だけ使っても暗号通信は可能である。その逆に、暗号化と復号化では暗号鍵を使い、分割と合成では暗号鍵を使わず単なる交互分割としてもよい。また、暗号鍵については、共通秘密鍵方式の例を説明したが、分割合成には共通秘密鍵を使い、暗号化復号化には公開鍵方式を使うことも可能である。

【００３１】２つの通信路を利用する例を説明したが、３つ以上の通信路を利用してもよいことは明らかである。４つに分割する時は、鍵の２ビットに対応して振り分け先を決める。同様にして鍵のｎビットを使用することで、2^nに分割することが可能である。2^{n-1}と2^nの間の数に分割したい場合は、鍵のｎビットを使用して、これを２進数としてみて、この数が分割したい数以上の場合は無視すればよい。例えば、３つに分割する場合はｎ＝２の場合であり、鍵のビットの並びは00，01，10，11の４つがある。10進数では、０，１，２，３であり、３以上である鍵のビット並び11のときを無視して、残りの３つに振り分けが可能である。受信側では、これを逆に行なって合成が可能である。共通鍵方式なので受信側で合成する場合も問題は生じない。

【００３２】上記のように、本発明の第１の実施の形態では、セキュア通信装置を、送りたい情報をデジタル化し、ビット列に変換した後、これを暗号化処理し、その後２つのデータに分割し、それぞれを２つの通信路で別々に送り、別々の通信路を介して受信した２つの暗号文を１つに合成してから復号して１つの平文を復元する構成にしたので、情報の盗聴が困難になるし、分割の片方を盗聴しても暗号解読はできない。

【００３３】（第２の実施の形態）本発明の第２の実施の形態は、送りたい秘密情報をデジタル化してビット列に変換した後、暗号化処理とデータ分割を一体として行ない、それぞれを２つの通信路で別々に送り、別々の通信路を介して受信した２つの暗号文を一つの平文に復元するセキュア通信装置である。

【００３４】図２は、本発明の第２の実施の形態のセキュア通信装置のシステム構成図である。図２において、暗号化装置１は、送信する平文のデータを、暗号化鍵で暗号化するとともに２つに分割する装置である。復号化装置２は、２つに分割された受信暗号化データを１つの平文に戻す装置である。通信路（Ａ）３は、第１の通信路である。通信路（Ｂ）４は、第２の通信路である。

【００３５】上記のように構成された本発明の第１の実施の形態のセキュア通信装置の動作を図２を使って説明する。図示していない装置で、送りたい情報をデジタル化し、ビット列データに変換する。変換したビット列データを、暗号鍵を使って暗号化装置１により暗号化すると同時に２つに分割する。

【００３６】暗号化と分割をまとめて行なう方法の一例として、ブロック暗号として有名なＤＥＳ方式を用いた例を示す。ＤＥＳは64ビット毎に処理していくが最終出力のところで左右の片側32ビットずつを取り出して２つに分けていく（図３参照）。これを逆にして合成・復号を行なう。

【００３７】通信路（Ａ）３では、一方の分割暗号化データを転送する。通信路（Ｂ）４では、他方の分割暗号化データを転送する。このように、情報を複数のデータに分け、それぞれを複数の通信路で別々に送る。この場合の複数の通信路とは、物理的に異なる通信路の場合の他、同じ無線であるが異なるチャンネルで送る場合、あるいは物理的に同じ通信路でも異なる時間に送る場合を含む。

【００３８】受信側では、送信側と逆の操作を行ない、２つの受信データの合成と復号化を行ない、元のメッセージを取り出す。復号化装置２では、通信路（Ａ）３と

通信路（Ｂ）４から暗号化データを受信し、受信した２つの暗号化ビット列を暗号鍵を使って合成すると同時に復号して平文に復元する。

【００３９】このように、暗号化の手法を使って、暗号化と分割を一体として行ない、合成と復号化を一体として行なう。１つのデータを暗号化と同時に分割して送信するので、一方の分割データを盗聴して解読しようとしても、全く意味のないデータしか得られず、秘密のデータが悪用される危険はない。２つの通信路を利用する例を説明したが、３つ以上の通信路を利用してもよいことは明らかである。

【００４０】上記のように、本発明の第２の実施の形態では、セキュア通信装置を、送りたい情報をデジタル化し、ビット列に変換した後、これを暗号化処理とデータ分割を一体として行ない、それぞれを２つの通信路で別々に送り、別々の通信路を介して受信した２つの暗号文から１つの平文を復元する構成にしたので、情報の盗聴が困難になるし、分割の片方を盗聴しても暗号解読はできない。

【００４１】（第３の実施の形態）本発明の第３の実施の形態は、秘密情報をデジタル化してビット列に変換した後、暗号化処理しながら、２つのデータに分割し、それぞれを２つの記憶装置に別々に格納し、別々の記憶装置から読み出した２つの暗号文を１つの平文に復元するセキュア記憶装置である。

【００４２】図４は、本発明の第３の実施の形態のセキュア記憶装置の構成図である。図４において、暗号化装置１は、記憶する平文のデータを、暗号化鍵で暗号化する装置である。復号化装置２は、暗号化データを平文に戻す装置である。記憶装置（Ａ）８は、第１の記憶装置である。記憶装置（Ｂ）９は、第２の記憶装置である。

【００４３】上記のように構成された本発明の第３の実施の形態のセキュア記憶装置の動作を図４を使って説明する。書込側では、図示しない装置で、記憶する秘密情報をデジタル化してビット列データに変換する。変換したビット列データを、暗号鍵を使って暗号化装置１により暗号化するとともに分割する。情報を２つに分割する時には、単純な交互分割を使ってもよいが、第２の実施の形態と同様に、暗号鍵を使って暗号化と分割を一体として行なう。こうして、１つのデータから２つに分割された暗号文が得られる。

【００４４】記憶装置（Ａ）８では、一方の分割データを記憶する。記憶装置（Ｂ）９では、他方の分割データを記憶する。このように、情報を２つのデータに分け、それぞれを２つの記憶装置に別々に格納する。この場合の２つの記憶装置とは、物理的に異なる記憶装置や記憶媒体でもよく、あるいは１つの記憶装置や記憶媒体の異なる記憶領域でもよい。物理的に異なった記憶装置や記憶媒体を用いる方が安全であるが、１つの記憶装置や記憶媒体の異なった領域を使う場合でも、記憶領域が秘密であれば、安全性に格別の問題はない。

【００４５】読出側では、書込側と逆の操作を行ない、２つの読出データの合成と復号を行ない、元のメッセージを取り出す。記憶装置（Ａ）８と記憶装置（Ｂ）９から暗号化データを読み出し、復号化装置２で、暗号鍵を使って２つの暗号化データを合成、復号して、もとの平文に復元する。

【００４６】このようにして、暗号化データを２つのデータに分割して記憶するので、一方の分割データを格納した記憶装置を盗んで解読しようとしても、全く意味のないデータしか得られず、秘密のデータが解読される危険はない。したがって、秘密のデータを安全に運搬あるいは保管できる。

【００４７】なお、通信の場合と同様に、３つ以上の暗号化データに分割して、３つ以上の記憶装置に記憶するようにしてもよい。また、第１の実施の形態と同様に、暗号化と分割、合成と復号を分離してもよい。

【００４８】上記のように、本発明の第３の実施の形態では、セキュア記憶装置を、記憶する情報をデジタル化し、ビット列に変換した後、これを暗号化処理しながら、２つのデータに分割し、それぞれを２つの記憶装置に別々に格納し、別々の記憶装置から読み出した２つの暗号文を１つの平文に復元する構成としたので、情報全体の盗難を困難にするとともに、一部の記憶装置が盗難にあっても、全部の記憶装置と復号鍵が盗まれない限り秘密がもれることはない。

【００４９】

【発明の効果】以上のように、本発明では、セキュア通信装置を、情報を単独では意味のない複数のデータに分ける分割手段と、それぞれのデータを複数の通信路で別々に送る送信手段とを具備する構成としたので、通信路を分けて情報の盗聴を困難にできるとともに、分割した一部のデータが盗聴されても全部が盗聴されない限り悪用されないという効果が得られる。

【００５０】また、分割手段に、暗号化鍵に応じてデータを複数に分割する暗号化手段を設けたので、暗号化鍵がない限り複数に分割されたデータを再構成できないという効果が得られる。

【００５１】また、暗号化手段は、送信データをデジタル化してビット列に変換する手段と、ビット列を暗号化鍵に応じて複数のビット列に分割する手段とを有する構成としたので、暗号化鍵がない限り複数に分割されたデータを再構成できないという効果が得られる。

【００５２】また、複数の通信路から別々に複数の暗号化データを受信する受信手段と、受信した複数の暗号化データを復号鍵により一つの平文に復号する復号手段とを設けたので、分割された複数の暗号化データを復号鍵により容易に再構成できるという効果が得られる。

【００５３】また、セキュア記憶装置を、情報を単独では意味のない複数のデータに分ける分割手段と、それぞ

れのデータを複数の記憶装置または１つの記憶装置の複数の異なる記憶領域に格納する書込手段とを具備する構成としたので、記憶装置を分けて情報の盗聴を困難にできるとともに、分割した一部の記憶装置が盗難にあっても全部が盗まれない限り悪用されないという効果が得られる。

【００５４】また、分割手段に、暗号化鍵に応じてデータを複数に分割する暗号化手段を設けたので、暗号化鍵がない限り複数に分割されたデータを再構成できないという効果が得られる。

【００５５】また、暗号化手段は、書込データをデジタル化してビット列に変換する手段と、ビット列を暗号化鍵に応じて複数のビット列に分割する手段とを有するので、暗号化鍵がない限り複数に分割されたデータを再構成できないという効果が得られる。

【００５６】また、複数の記憶装置または１つの記憶装置の複数の異なる記憶領域から別々に複数の暗号化データを読み出す読出手段と、読み出した複数の暗号化データを復号鍵により１つの平文に復号する復号手段とを設けたので、分割された複数の暗号化データを復号鍵により容易に再構成できるという効果が得られる。

＊【図面の簡単な説明】

【図１】本発明の第１の実施の形態のセキュア通信装置の構成図、

【図２】本発明の第２の実施の形態のセキュア通信装置の構成図、

【図３】本発明の第２の実施の形態のセキュア通信装置で用いる暗号化装置の構成図、

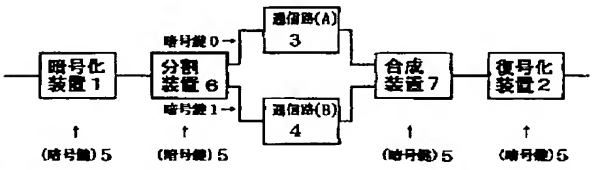
【図４】本発明の第３の実施の形態のセキュア記憶装置の構成図、

【図５】従来の暗号通信システムの構成図である。

【符号の説明】

1　暗号化装置
2　復号化装置
3　通信路（Ａ）
4　通信路（Ｂ）
5　暗号鍵
6　分割装置
7　合成装置
8　記憶装置（Ａ）
9　記憶装置（Ｂ）
10　通信路

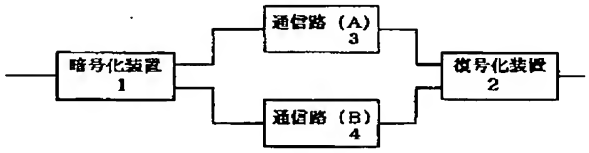
【図１】



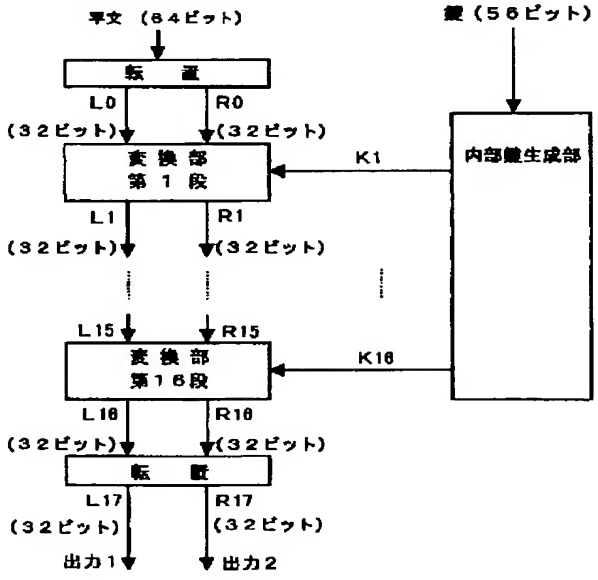
分割動作説明
暗号出力例 11011001 → ０側出力 1001
暗号鍵例 01011010 → １側出力 1110

合成動作説明
０側出力例 1001 → 暗号鍵例 01011010
１側出力例 1110 → 復号入力 11011001

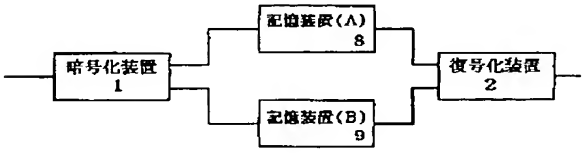
【図２】



【図３】



【図４】



【図５】